

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ «КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО» ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

ЛАБОРАТОРНА РОБОТА №1

3 дисципліни «Криптографія»

Виконали:

студенти 3 курсу ФТІ групи ФБ-93 Абдуллаєва Есміра Шовак Мирослав

Викладач:

Селюх П. В.

Мета роботи: засвоєння понять ентропії на символ джерела та його надлишковості, вивчення та порівняння різних моделей джерела відкритого тексту для наближеного визначення ентропії, набуття практичних навичок щодо оцінки ентропії на символ джерела.

Завдання

- 1. Написати програми для підрахунку частот букв і частот біграм в тексті, а також підрахунку Н1 та Н2 за безпосереднім означенням. Підрахувати частоти букв та біграм, а також значення Н1 та Н2 на довільно обраному тексті російською мовою достатньої довжини (щонайменше 1Мб), де імовірності замінити відповідними частотами. Також одержати значення Н1 та Н2 на тому ж тексті, в якому вилучено всі пробіли.
 - 2. За допомогою програми CoolPinkProgram оцінити значення H (10), H (20), H (30).
- 3. Використовуючи отримані значення ентропії, оцінити надлишковість російської мови в різних моделях джерела.

Хід роботи та опис труднощів:

Під час роботи , з огляду на вимоги форматування тексту , та різних операцій над ним , було вирішено використовувати мову руthon. У якості вхідного тексту була обрана книга "Зелена миля". Форматування вхідного тексту не викликало значних труднодщів . За допомогою стандартних функцій ми змогли позбутися пробілів , твердого знаку , змінити всі великі букви на малі. За допомогою регулярного виразу змогли досягнути зчитування з файлу тільки алфавіту. Для зручнішого використання програми , в залежності від завдання , було вирішено зробити лаконічне меню з 4 можливостями : зчитування файлу з пробілами і виконання операцій над знаками , зчитування файлу без пробілів , аналогічно було проведено для біграм. Сортування монограм ми досягли за допомогою питру. Труднощі виникли при створення функції для зчитування біграм. Було прийнято рішення створити масив букв , і вже до значень цього масиву додавати ,як аргумент фукції ще одну букву по черзі і потім робити зчитування циклічно для кожної отриманої пари. Вивід реалізовували у вигляді квадратної матриці , для презентабельного вигляду ми відформатували значення наших Н2 до трьох знаків після коми.

Код програми

```
import math
                                                  r = [alphabet[a] + i]
                                                  for j in r:
import re
import numpy as np
                                                      letter = one.count(j)
                                                      if letter == 0:
file =
open ("/Users/esmira.23/Desktop/КПИ
                                                         y1 = 0
/3курс/Крипта/1.txt", "r")
                                                      else:
data =
                                                          y1 = -
file.read().replace("ъ","ь")
                                         math.log2(letter/number)
one = re.sub(r"[^a-\pi]+", "",
                                                      H2 = letter/number *
data.lower()).replace("ъ","ь").rep
                                         у1
lace("ë", "e")
                                                      save1.append("%.3f" %
                                         H2)
# m=32 - кількість букв алфавіту
                                                      save3.append(H2)
alphabet =
                                                      save2.append(i)
['a','б','в','г','д','е','ж','з','
                                             print(alphabet[a], "
и','й','к','л','м','н','о','п','р'
                                         ".join(map(str, save1)))
,'C','T','Y','Ф','X','Ц','Ч','Ш','
                                             save1.clear()
щ','ы','ь','э','ю','я',' ']
save = []
                                          if ans == "1":
save1 = []
                                             number = len(one)
save2 = []
                                             func()
save3 = []
                                         elif ans == "2":
save4 = []
                                             one = one.replace(" ", "")
                                             number = len(one)
print("1. First task\n2. Second
                                             func()
task\n3. Third task\n4. Fourth
                                         elif ans == "3":
task\n")
                                             number = len(one)
ans = input()
                                             arr =
                                          [0,1,2,3,4,5,6,7,8,9,10,11,12,13,1
                                         4,15,16,17,18,19,20,21,22,23,24,24
def func():
                                          ,26,27,28,29,30,31]
    for i in alphabet:
                                             print(" ", "
        letter = one.count(i)
        if letter == 0:
                                          ".join(alphabet))
                                             for item in arr:
            \lambda = 0
        else:
                                                 bigram(item)
            y = -
                                             print("H2: ", (sum(save3)/2))
                                         elif ans == "4":
math.log2(letter/number)
                                             one = one.replace(" ", "")
        H1 = letter/number * y
        save.append(H1)
                                             number = len(one)
        save1.append(i)
                                             arr =
        save4.append("%.4f" % H1)
                                         [0,1,2,3,4,5,6,7,8,9,10,11,12,13,1
    a =
                                         4,15,16,17,18,19,20,21,22,23,24,24
                                          ,26,27,28,29,30,31]
np.column stack([save1,save4])
                                             print(" ", "
    b = sorted(a, key = lambda x:
                                         ".join(alphabet))
    c = "\n".join(map(str,b))
                                             for item in arr:
                                                 bigram(item)
    print(c)
    print("H1: ", (sum(save)))
                                             print("H2: ", (sum(save3)/2))
                                         else:
def bigram(a):
                                             print("Wrong input")
    for i in alphabet:
```

Значення Н1 для тексту з пробілами:

Значення Н1 для тексту без пробілів:

эначения 111 для тексту з прооглами.	эначения пт для тексту о
['ф' '0.0193']	['''0.0000']
['ц' '0.0209']	['ф' '0.0225']
['щ' '0.0227']	['ц' '0.0245']
['э' '0.0308']	['щ' '0.0265']
['ю' '0.0364']	['э' '0.0360']
['x' '0.0519']	['ю' '0.0425']
['ш' '0.0522']	['x' '0.0603']
['й' '0.0579']	['ш' '0.0607']
['ж' '0.0628']	['й' '0.0672']
['ч' '0.0832']	['ж' '0.0729']
['3' '0.0871']	['ч' '0.0961']
['6' '0.0872']	['3' '0.1006']
['ы' '0.0900']	['6' '0.1007']
['r' '0.0905']	['ы' '0.1039']
['ь' '0.0919']	['r' '0.1044']
['я' '0.1091']	['ь' '0.1060']
['n' '0.1303']	['я' '0.1255']
['y' '0.1369']	['п' '0.1495']
['д' '0.1393']	['y' '0.1568']
['m' '0.1428']	['д' '0.1596']
['ĸ' '0.1528']	['m' '0.1634']
['в' '0.1571']	['ĸ' '0.1746']
['p' '0.1746']	['B' '0.1795']
['c' '0.1937']	['p' '0.1990']
['л' '0.2004']	['c' '0.2200']
['T' '0.2171']	['л' '0.2274']
['и' '0.2238']	['т' '0.2458']
['н' '0.2264']	['и' '0.2530']
['a' '0.2546']	['н' '0.2559']
['e' '0.2624']	['a' '0.2865']
['o' '0.3227']	['e' '0.2948']
[' ' '0.4372']	['o' '0.3586']
H1: 4.366187862436842	H1: 4.474445521025726

Значення Н2 з пробілами:

H2: 3.980088273281425

0.017 0.011 0.010 0.029 0.001 0.006 0.039 0.059 0.023 0.022 0.021 0.010 0.010 0.007 0.000 0.000 0.000 0.010 0.014 0.008 0.021 0.000 0.027 0.030 0.002 0.001 0.001 6 0.008 0.000 0.001 0.000 0.000 0.015 0.000 0.000 0.011 0.000 0.003 0.008 0.000 0.003 0.020 0.000 0.016 0.001 0.000 0.010 0.000 0.000 0.000 0.000 0.000 0.002 0.028 0.002 0.000 0.000 0.006 0.003 0.032 0.000 0.000 0.005 0.000 0.001 0.000 0.004 0.033 0.005 0.023 0.002 0.002 0.012 0.038 0.003 0.008 0.022 0.003 0.006 0.000 0.000 0.000 0.001 0.000 0.000 0.000 0.016 0.002 0.000 0.000 0.006 0.000 0.003 0.016 0.000 0.003 0.051 0.000 0.007 0.000 0.000 0.007 0.000 0.000 0.000 0.001 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.009 0.008 д 0.035 0.009 0.014 0.000 0.020 0.000 0.007 0.015 0.026 0.002 0.002 0.017 0.003 0.000 0.000 0.001 0.041 0.003 0.001 0.001 0.008 0.000 0.001 0.000 e 0.001 0.011 0.029 0.019 0.011 0.008 0.011 0.001 0.015 0.013 0.046 0.029 0.045 0.001 0.008 0.052 0.028 0.037 0.001 0.001 0.005 0.003 0.010 0.008 0.000 0.000 0.000 0.001 0.002 0.101 0.010 0.009 ĸ 0.012 0.007 0.000 0.015 0.000 0.000 0.008 0.008 0.003 0.000 0.000 0.000 0.000 0.001 0.000 0.000 0.028 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.001 0.000 0.000 0.003 3 0.042 0.001 0.007 0.004 0.008 0.004 0.001 0.000 0.004 0.000 0.002 0.002 0.002 0.016 0.005 0.000 0.003 0.000 0.000 0.004 0.000 0.000 0.000 0.000 0.000 0.000 0.004 0.002 0.000 0.000 0.003 0.017 0.002 0.002 0.015 0.005 0.016 0.012 0.003 0.018 0.004 0.009 0.016 0.043 0.019 0.027 0.002 0.002 0.008 0.022 0.027 0.000 0.001 0.012 0.007 й 0.000 0.000 0.000 0.002 0.000 0.000 0.000 0.000 0.000 0.002 0.000 0.001 0.004 0.000 0.000 0.000 0.004 0.003 0.000 0.000 0.000 0.001 0.003 0.001 0.000 0.000 0.000 0.000 0.000 0.000 0.048 0.000 0.000 0.000 к 0.053 0.002 0.000 0.001 0.007 0.000 0.000 0.023 0.000 0.008 0.000 0.004 0.057 0.019 0.001 0.006 0.017 0.000 0.000 0.001 0.000 0.000 0.000 0.000 n A. A42 0.001 0.000 0.002 0.001 0.035 0.003 0.003 8.845 0.000 0.004 0.005 0.000 8.883 A. 843 0.000 0.000 0.017 0.881 0.011 0.000 0.000 0.000 A.AA1 0.000 0.000 0.008 0.028 0.000 0.009 0.014 0.072 м 0.022 0.000 0.000 0.016 0.000 0.053 0.000 0.000 0.023 0.000 0.017 0.033 0.018 0.000 0.000 0.032 0.000 0.001 0.001 0.001 0.000 0.000 н 0.067 0.004 0.005 0.061 0.000 0.001 0.043 0.000 0.005 0.000 0.000 0.017 0.065 0.000 0.001 0.003 0.006 0.025 0.001 0.000 0.004 0.003 0.000 0.001 0.023 0.012 0.000 0.003 0.016 0.039 0.000 0.000 0.038 0.011 0.003 0.000 0.000 0.042 0.031 0.016 0.019 0.011 0.009 0.030 0.021 0.041 0.041 0.054 0.002 0.011 0.038 0.048 0.001 0.008 0.007 0.001 0.019 0.000 0.001 0.003 0.125 0.026 n 0.015 0.000 0.000 0.000 0.000 0.023 0.000 0.000 0.009 0.000 0.002 0.008 0.000 0.002 0.070 0.001 0.043 0.000 0.881 0.008 0.000 0.000 0.000 0.000 0.000 0.000 0.004 0.001 0.000 0.000 0.004 0.001 0.000 0.013 p 0.046 0.032 0.001 9.994 8.881 0.002 0.001 0.003 0.039 0.003 0.001 0.036 0.000 0.004 0.001 0.010 0.045 0.001 0.005 0.013 0.010 0.000 0.001 0.000 0.001 c 0.012 0.001 0.012 0.000 0.004 0.028 0.001 0.000 0.023 0.000 0.024 0.027 0.013 0.011 0.020 0.016 0.002 0.007 0.868 0.006 0.000 0.002 0.001 0.003 0.001 0.000 0.003 0.022 0.001 0.002 0.031 0.027 т 0.042 0.001 0.000 0.000 0.088 0.003 0.015 0.000 0.000 0.000 0.000 0.014 0.040 8.881 0.002 0.045 0.001 0.015 0.000 0.035 0.000 0.026 0.007 0.002 0.002 0.008 0.002 0.022 0.009 0.000 0.001 0.003 0.000 0.002 v 0.006 0.009 0.008 0.889 0.014 0.001 0.012 0.004 0.000 0.002 0.010 0.018 0.012 0.003 0.005 0.006 0.007 0.013 0.821 0.000 0.000 0.004 0.000 0.009 0.006 0.000 0.009 0.001 0.008 0.001 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 × 0.009 0.000 0.003 0.000 0.000 0.000 0.000 0.000 0.002 0.000 0.000 0.002 0.000 0.003 0.021 0.000 0.003 0.000 0.000 0.002 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.003 0.000 0.023 0.000 0.000 0.002 0.000 0.000 ц 0.005 0.000 0.001 0.000 0.000 0.000 0.000 0.003 0.000 0.000 0.000 0.004 0.000 0.002 0.000 0.000 0.000 0.000 0.002 0.003 0.000 0.000 ч 0.018 0.000 0.000 0.000 0.000 0.028 0.000 0.000 0.013 0.000 0.005 0.000 0.000 0.008 0.001 0.000 0.000 0.000 0.032 0.006 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.009 0.000 0.000 0.000 0.001 0.000 0.011 0.001 0.003 0.005 0.003 0.019 0.002 0.000 0.000 0.009 0.000 w 0.007 0.000 0.000 0.000 0.000 0.019 0.000 0.000 0.011 0.000 0.007 0.007 0.001 0.003 0.005 0.000 0.000 0.000 0.002 0.003 0.000 0.000 0.000 0.000 0.009 0.000 0.000 0.000 0.000 0.038 ы 0.000 0.001 0.001 0.001 0.000 0.013 0.018 0.011 0.002 0.000 0.007 0.000 0.000 0.000 0.000 0.007 0.000 0.000 0.000 0.000 0.004 ь 0.000 0.000 0.000 0.000 0.001 0.003 0.000 0.001 0.000 0.000 0.009 0.000 0.003 0.012 0.000 0.000 0.000 0.007 0.001 0.000 0.000 0.000 0.002 0.001 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 ю 0.000 0.003 0.000 0.000 0.004 0.000 0.001 0.000 0.000 0.000 0.001 0.000 0.000 0.000 0.000 0.000 0.002 0.002 0.003 0.000 0.000 0.001 0.000 0.003 0.000 0.003 0.000 0.000 0.000 0.001 0.001 0.043 0.010 0.017 0.051 0.084 0.028 0.062 0.033 0.013 0.036 0.062 0.000 0.067 0.021 0.057 0.098 0.071 0.106 0.033 0.096 0.058 0.037 0.004 0.021 0.004

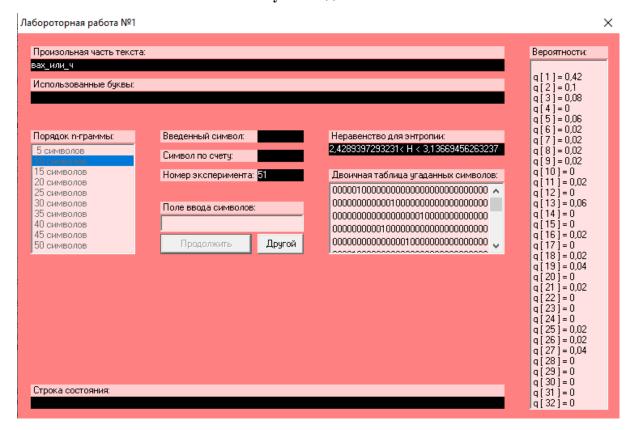
Значення Н2 без пробілів:

H2: 4.1878402723119

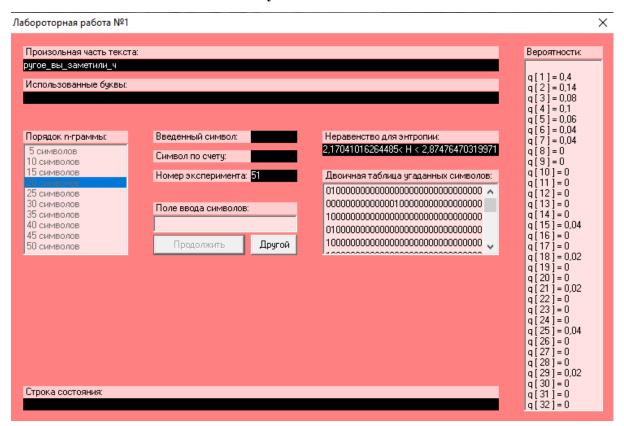
a 0.003 0.016 0.034 0.009 0.028 0.018 0.013 0.037 0.011 0.007 0.053 0.071 0.035 0.040 0.013 0.028 0.028 0.044 0.041 0.008 0.002 0.013 0.002 0.014 0.010 0.004 0.000 0.000 0.005 0.012 0.020 0.002 0.004 0.009 0.003 0.023 0.019 0.000 0.011 0.002 5 0.009 0.000 0.001 0.000 0.000 0.017 0.000 0.000 0.013 0.000 0.001 0.000 0.000 0.000 0.000 0.000 0.032 0.002 0.000 0.007 в 0.038 0.004 0.003 0.004 0.008 0.039 0.001 0.008 0.029 0.000 0.008 0.008 0.005 0.017 0.047 0.009 0.011 0.031 0.010 0.008 0.000 0.001 0.001 0.002 0.006 0.000 0.020 0.002 0.003 0.000 0.004 0.000 0.010 0.001 0.000 0.019 0.002 0.000 0.001 0.007 0.000 0.004 0.019 0.001 0.005 0.059 0.002 0.002 0.001 0.009 0.000 0.000 0.001 0.000 0.000 д 0.041 0.001 0.011 0.001 0.002 0.048 0.017 0.001 0.024 0.000 0.005 0.009 0.001 0.020 0.030 0.002 0.010 0.005 0.002 0.020 0.000 0.001 0.003 0.001 0.001 0.000 0.007 0.006 0.003 0.001 0.005 0.000 e 0.003 0.016 0.018 0.023 0.056 0.001 0.009 0.003 0.020 0.026 0.037 0.029 0.011 0.019 0.010 0.040 0.063 0.014 0.027 0.063 0.044 0.049 0.008 0.016 0.013 0.010 0.000 0.002 0.007 ж 0.014 0.000 0.000 0.000 0.008 0.032 0.000 0.000 0.018 0.000 0.004 0.000 0.000 0.010 0.009 0.000 0.000 0.000 0.000 0.004 0.000 0.000 0.000 0.001 0.000 0.000 0.000 0.001 0.000 0.000 0.000 0.000 0.002 0.005 0.004 0.003 0.021 0.007 0.003 0.002 0.005 0.000 0.000 и 0.005 0.013 0.033 0.009 0.028 0.019 0.005 0.025 0.016 0.011 0.027 0.051 0.029 0.046 0.016 0.024 0.013 0.041 0.039 0.008 0.002 0.017 0.008 0.014 0.008 0.001 0.000 0.000 0.004 0.003 0.015 0.000 0.001 й 0.002 0.004 0.006 0.003 0.007 0.001 0.002 0.002 0.006 0.000 0.009 0.002 0.007 0.010 0.005 0.005 0.011 0.006 0.002 0.001 0.001 0.005 0.002 0.000 0.000 к 0.062 0.003 0.006 0.002 0.005 0.010 0.002 0.002 0.030 0.000 0.005 0.010 0.005 0.009 0.068 0.006 0.023 0.007 0.010 0.021 0.000 0.001 0.001 0.003 0.000 0.000 0.000 0.000 0.002 0.000 0.002 0.000 0.049 0.001 0.010 0.008 0.004 0.006 0.056 0.000 0.012 0.007 0.015 0.055 0.011 0.027 0.006 0.016 0.003 0.000 0.010 0.001 м 0.027 0.004 0.007 0.003 0.006 0.038 0.001 0.002 0.031 0.000 0.007 0.003 0.005 0.026 0.041 0.011 0.003 0.011 0.004 0.022 0.000 0.001 0.000 0.005 0.001 0.000 0.018 0.001 0.002 0.000 0.010 0.000 0.010 0.001 0.078 0.004 0.006 0.008 0.072 0.001 0.003 0.053 0.000 0.001 0.002 0.025 0.078 0.002 0.011 0.009 0.031 0.002 0.005 0.001 0.014 0.003 0.019 0.002 0.038 0.062 0.047 0.044 0.023 0.024 0.018 0.019 0.035 0.033 0.050 0.055 0.076 0.019 0.033 0.048 0.061 0.065 0.008 0.010 0.011 0.002 0.030 0.014 0.003 0.000 0.000 0.007 0.003 0.016 0.000 0.002 0.001 p 0.053 0.003 0.006 0.002 0.006 0.046 0.004 0.001 0.043 0.000 0.006 0.002 0.005 0.012 0.053 0.002 0.007 0.016 0.012 0.037 0.000 0.002 0.000 0.002 0.002 0.000 0.015 0.007 0.002 0.002 0.011 0.000 c 0.014 0.003 0.002 0.007 0.033 0.002 0.001 0.028 0.000 0.030 0.031 0.017 0.016 0.025 0.021 0.003 0.011 0.071 0.009 0.000 0.004 0.001 0.004 0.001 0.000 0.025 0.003 0.037 т 0.050 0.003 0.022 0.002 0.005 0.042 0.001 0.002 0.033 0.000 0.011 0.004 0.006 0.015 0.104 0.009 0.027 0.017 0.008 0.019 0.001 0.001 0.001 0.004 0.001 0.000 0.016 0.046 0.002 0.003 0.009 0.000 0.007 0.015 0.013 0.020 0.027 0.000 0.000 φ 0.001 0.000 0.000 0.000 0.000 0.002 0.000 0.000 0.010 0.000 0.000 0.001 0.000 0.000 0.003 0.000 0.002 0.001 0.000 0.001 0.008 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 x 0.011 0.001 0.003 0.001 0.000 0.001 0.005 0.000 0.002 0.003 0.002 0.006 0.025 0.004 0.004 0.001 0.003 0.000 0.000 0.000 0.000 ц 0.006 0.000 0.001 0.000 0.000 0.009 0.000 0.000 0.004 0.000 0.001 0.000 0.000 0.001 0.004 0.000 0.000 0.000 0.000 0.003 0.000 0.000 0.000 0.000 0.000 0.000 0.002 0.000 0.000 0.000 0.000 0.000 0.000 0.006 0.010 0.002 0.038 0.008 0.000 0.000 w 0.008 0.000 0.001 0.000 0.000 0.022 0.000 0.000 0.013 0.000 0.008 0.008 0.001 0.003 0.006 0.000 0.000 0.000 0.002 0.004 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.011 0.000 0.000 0.000 0.000 0.022 0.000 0.013 0.000 0.008 0.008 0.001 0.003 0.006 0.000 0.000 0.000 0.002 0.004 0.000 0.000 0.000 0.000 0.000 ы 0.001 0.005 0.013 0.002 0.005 0.011 0.001 0.003 0.004 0.015 0.004 0.021 0.015 0.008 0.005 0.010 0.004 0.011 0.010 0.003 0.000 0.010 0.000 0.004 0.011 0.000 0.000 0.000 0.001 0.000 0.002 0.000 0.016 0.023 э 0.000 0.000 0.000 0.000 0.003 0.000 0.000 0.000 0.000 0.001 0.000 0.007 0.001 0.001 0.000 0.000 0.002 0.000 0.027 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 0.000 я 0.002 0.006 0.017 0.004 0.014 0.004 0.003 0.008 0.009 0.000 0.009 0.015 0.009 0.022 0.010 0.018 0.004 0.018 0.020 0.007 0.000 0.004 0.001 0.006 0.001 0.003 0.000 0.000 0.002 0.002 0.004 H2: 4.1878402723119

За допомогою програми CoolPinkProgram оцінили значення $H^{(10)}$, $H^{(20)}$, $H^{(30)}$. У кожному досліді було зроблено не менше ніж 50 експериментів.

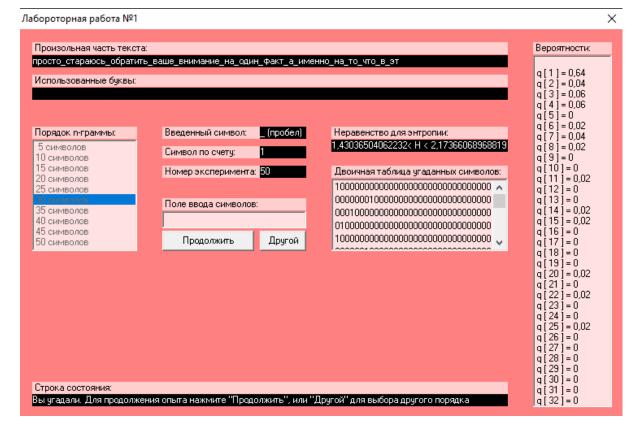
Результат для H⁽¹⁰⁾



Результат для H⁽²⁰⁾



Результат для H⁽³⁰⁾



Результат надлишковості російської мови

$$Had$$
лишковість джерела відкритого тексту (мови) дорівнює $R=1-\frac{H_{\infty}}{H_{0}}$

$$H_0 = log_2 32 = 5$$

$$1-(2.428/5)=0.5144>R^{(10)}>1-(3.136/5)=0.3728$$

Аналогічні дії повели і для інших випадків.

$$0.566 > R^{(20)} > 0.4252$$

Висновки: під час лабораторної роботи, ми закріпили свої знання стосовно етропії та надлишковості тексту. Вирахували значення для вхідного тексту для монограм та біграм. Удосконалили свої знання мови руthon для роботи з різними структурами даних та файлами, навчилися краще придумовувати алгоритми для роботи з вхідним текстом.